CS4331/CS5342 Network Security
Homework 1

Submitted by:
Venkata Nikhil Thanikella
R11904730

Q.1. False (F) or True (T) and justify the answer (27 points)

1. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.

   False. 56 bits are used for encryption and the other 8 bits are for parity.

2. 4 keys does the Triple DES algorithm use?

   False. Triple DES uses 3 keys for encryption.

3. Like DES, AES also uses Feistel Structure.

   False. It uses substitution-permutation network.

4. There is an addition of round key before the start of the AES round algorithms.

   True. It's used to obscure the initial data before encryption starts.

5. If the sender and receiver use different keys, the system is referred to as conventional cipher system.

   False. It's called asymmetric key cryptography.

6. Symmetric Block Cypher provides authentication and confidentiality.

   True. AES is an example. It protects critical information.

7. Plain text is the data after encryption is performed.

   False. It's the original data before encryption is performed.

8. X.800 architecture was developed as an international standard and focuses on security in the context of networks and communications.

   True. It establishes guidelines and constraints to improve security during communication between nodes on a network and between the networks as well.

9. Data integrity assures that information and programs are changed only in a specified and authorized manner.

True. It ensures that data is not manipulated without permission and can be changed only in a certain way.

Q.2. Short answer Questions (21 points)

1. Release of message contents and traffic analysis are two types of **passive** attacks.
2. Replay, masquerade, modification of messages, and denial of service are example of **active** attacks.
3. A **block cipher** processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.
4. A **stream cipher** processes the input elements continuously, producing output one element at a time?
5. With the use of symmetric encryption, the principal security problem is to maintain the secrecy of **encryption key.**
6. AES's advantage is that most operations can be combined into **bitwise XOR** and **table lookups**.
7. What is the entropy of a uniform random distribution over 16 values **4 bits**.

Q.3. List and briefly define the three main basic security requirements (5 points)

They are confidentiality, integrity, and availability.

- Confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- Data integrity assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.
- Availability assures that systems work promptly, and service is not denied to authorized users, ensuring timely and reliable access to and use of information.

Q.4. What is symmetric encryption? What are the five ingredients? (5 points)

If sender and receiver share a common/same key, it is known as symmetric encryption.

The five ingredients are:

- **Plaintext**: the original message or data
- **Encryption algorithm**: performs various substitutions and transformations on the plaintext
- **Secret key:** key for encrypting the message.
- **Ciphertext**: the encrypted or encoded message.
- **Decryption algorithm**: takes the ciphertext and the same secret key and produces the original plaintext.

Q.5. What are unconditional security and computational security? (5 points)

1. Unconditional security: Even with unlimited computational resources, the cipher remains unbreakable because the ciphertext doesn't contain enough information to identify the plaintext.

2. Computational security: Breaking the cipher is either too expensive or would take longer than the information's relevance, making decryption impractical.

Q.6. What are Shannon's Diffusion and Confusion and corresponding methods to achieve them? (5 points)

Confusion: how does changing a bit of the key affect the ciphertext.
Diffusion: how does changing one bit of the plaintext affect the ciphertext.

Q.7. What are the criteria to evaluate a cipher, such as AES? (6 points)

The criteria to evaluate a cipher like AES include:

1. Security: The cipher should resist all known attacks, including brute force, cryptanalysis, and side-channel attacks.
2. Restricted space environments
3. Encryption vs decryption
4. Key Length and agility: Longer keys provide stronger security. AES supports 128, 192, and 256-bit keys for varying security levels.
5. Performance/Speed: The encryption and decryption processes should be efficient in terms of time and computational resources.
6. Software/Hardware Implementations and flexibility: The cipher should work across different hardware and software environments, with the ability to handle various data sizes.
7. Simplicity: The design should be easy to understand and implement, reducing the chance of errors or vulnerabilities.
8. Resistance to Known Attacks: The cipher should specifically resist attacks like differential and linear cryptanalysis, which target weaknesses in block ciphers.
9. Potential for instruction-level parallelism

Q.8. What are the properties of true random numbers? (6 points)

1. **Randomness**: Uniform Distribution and Independence; **Uniform Distribution**: Each possible value has an equal probability of occurrence, leading to a balanced representation of values. **Independence**: Each number is generated independently, meaning the generation of one number does not affect the generation of another.
2. **Unpredictable**: Future values cannot be predicted based on past values, ensuring randomness.

Q.9. What are Pseudorandom Number Generator's (PRNG) properties? (6 points)

The properties of Pseudorandom Number Generators (PRNGs) include:

1. Correctness: PRNGs should generate outputs that appear random and meet statistical properties of randomness, such as uniform distribution and independence.
2. Efficiency: The generation process should be computationally efficient, allowing rapid generation of numbers without consuming excessive resources.

3. Security: The PRNG should be secure against attacks, meaning its output cannot be feasibly predicted or reverse-engineered by an adversary.
4. Rollback Resistance: The PRNG should resist rollback attacks, where an attacker could revert to a previous state of the generator to predict future outputs.

Q.10. Consider a very simple symmetric block encryption algorithm in which 64-bits blocks of plaintext are encrypted suing a 128-bit key. Encryption is defined as

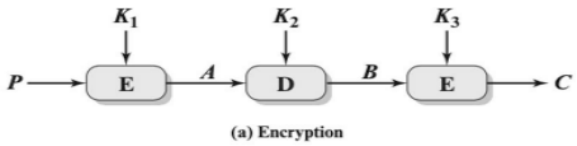
$$C = (P \oplus K0) \boxplus K1$$

Where C = ciphertext, K = secret key, K0 = leftmost 64 bits of K, K1 = rightmost 64 bits of K, $\oplus$ = bitwise exclusive OR, and $\boxplus$ is addition mod 264, Show the decryption equation. That is show the equation for P as a function of C, K0 and K1. (7 points)

- ⇨ C = (P $\oplus$ K0) $\boxplus$ K1
- ⇨ C $\boxplus$ K1 = P $\oplus$ K0 (reverse modulo)
- ⇨ P = (C $\boxplus$ K1) $\oplus$ K0 (XOR both sides with K0)

So, the decryption equation (to find plain text) is **P = (C $\boxplus$ K1) $\oplus$ K0**

Q.11. Figure shows the Triple DES encryption process. P is plaintext. C is ciphertext. (7 points)



(a) Encryption

(1) Write decryption equation.
(2) Write encryption equation.

This is a Triple DES so,

1. Decryption equation is P=D(K1,E(K2,D(K3,C)))
2. Encryption equation is C=E(K3,D(K2,E(K1,P)))